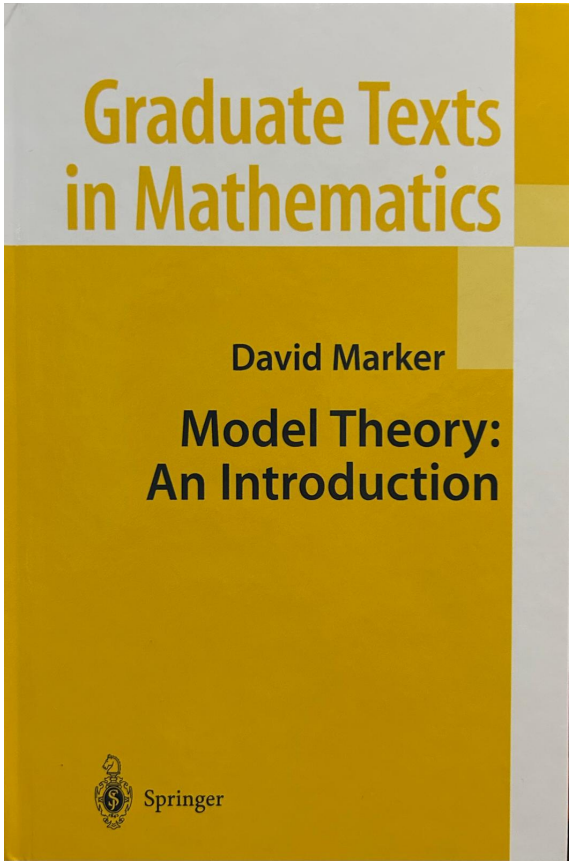
# Introdução à Teoria de Modelos e Aplicações

Eduardo Magalhães




https://link.springer.com/book/10.1007/b98860

Errata:

- https://homepages.math.uic.edu/~marker/mt-errors.html
- https://people.math.wisc.edu/~slempp/teach/Marker-errata.html

# Linguagens de Primeira Ordem

## Definição

*Uma linguagem de primeira ordem é dada por:*
*Símbolos Lógicos:*

- *Número contável de variáveis* $v_1, v_2, ...;$
- *Símbolo de igualdade* $=;$
- *Os conectivos lógicos* $\neg, \wedge, \vee, \rightarrow, \leftrightarrow;$
- *Os quantificadores* $\forall, \exists;$
- *Parêntese* $(,)$ *e virgula* $,$ .

*Símbolos não lógicos:*

- *Um conjunto* $\mathcal{C}$ *de símbolos constantes;*
- *Para cada* $n > 0$, *um conjunto* $\mathcal{F}_n$ *de símbolos funcionais n-ários;*
- *Para cada* $n > 0$, *um conjunto* $\mathcal{R}_n$ *de símbolos relacionais n-ários.*

# $\mathcal{L}$-estruturas

## Definição

*Dada uma LPO $\mathcal{L} = ((\mathcal{F}_n)_n, (\mathcal{R}_n), \mathcal{C})$, uma $\mathcal{L}$-estrutura $\mathcal{M}$ é dada por:*

- *Um conjunto não vazio $M$ chamado o domínio ou universo de $\mathcal{M}$;*
- *Para cada $f \in \mathcal{F}_n$, uma função $f^{\mathcal{M}} : M^n \to M$;*
- *Para cada $R \in \mathcal{R}_n$, uma relação $R^{\mathcal{M}} \subseteq M^n$;*
- *Para cada $c \in \mathcal{C}$, uma constante $c^{\mathcal{M}} \in M$.*

# Morfismos

## Definição

*Sejam $\mathcal{M}, \mathcal{N}$ duas $\mathcal{L}$-estruturas.*
*Um mapa $\pi : M \to N$ é um homomorfismo de $\mathcal{M}$ em $\mathcal{N}$ se:*

- *Para cada $R \in \mathcal{R}_n$, $(a_1, ..., a_n) \in R^{\mathcal{M}} \implies (\pi(a_1), ..., \pi(a_n)) \in R^{\mathcal{N}}$;*
- *Para cada $f \in \mathcal{F}_n$, $\pi(f^{\mathcal{M}}(a_1, ..., a_n)) = f^{\mathcal{N}}(\pi(a_1), ..., \pi(a_n))$;*
- *Para cada $c \in \mathcal{C}$, $\pi(c^{\mathcal{M}}) = c^{\mathcal{N}}$.*

*Um mapa $\pi : M \to N$ é um mergulho de $\mathcal{M}$ em $\mathcal{N}$ se:*

- *$\pi$ é um homomorfismo injetivo;*
- *Para cada $R \in \mathcal{R}_n$, $(a_1, ..., a_n) \in R^{\mathcal{M}} \iff (\pi(a_1), ..., \pi(a_n)) \in R^{\mathcal{N}}$;*

*Um isomorfismo é um mergulho bijetivo.*

## Definição

*Sejam $\mathcal{M}, \mathcal{N}$ duas $\mathcal{L}$-estruturas com $M \subseteq N$. Dizemos que $\mathcal{M}$ é uma subestrutura de $\mathcal{N}$, ou que $\mathcal{N}$ é uma extensão de $\mathcal{M}$, denotado por $\mathcal{M} \leq \mathcal{N}$, se a inclusão $\iota : M \hookrightarrow N$ for um mergulho.*

# $\mathcal{L}$-Termos

## Definição

*Seja $\mathcal{L}$ uma LPO. Um $\mathcal{L}$-termo é uma $\mathcal{L}$-palavra definida de acordo com as seguintes regras:*

- *Para cada $n > 0$, $v_n$ é um $\mathcal{L}$-termo;*
- *Para cada $c \in \mathcal{C}$, $c$ é um $\mathcal{L}$-termo;*
- *Para cada $f \in \mathcal{F}_n$ e $\mathcal{L}$-termos $t_1, ..., t_n$, $f(t_1, ..., t_n)$ é um $\mathcal{L}$-termo;*
- *Qualquer $\mathcal{L}$-termo é obtido da aplicação destas regras um número finito de vezes.*

## Definição

*Uma $\mathcal{L}$-formula atómica é dada por:*

- *$t_1 = t_2$ onde $t_1, t_2$ são $\mathcal{L}$-termos;*
- *$R(t_1, ..., t_n)$, para algum $R \in \mathcal{R}_n$ e termos $t_1, ..., t_n$.*

# $\mathcal{L}$-fórmulas

## Definição

*Uma $\mathcal{L}$-formula é definida recursivamente de acordo com as seguintes regras:*

- *Qualquer $\mathcal{L}$-formula atómica é uma $\mathcal{L}$-fórmula;*
- *Se $\phi$ é uma $\mathcal{L}$-fórmula, então $\neg\phi$ é uma $\mathcal{L}$-fórmula;*
- *Se $\phi, \psi$ são $\mathcal{L}$-fórmulas, então $\phi \wedge \psi$, $\phi \vee \psi$, $\phi \rightarrow \psi$ e $\phi \leftrightarrow \psi$ são $\mathcal{L}$-fórmulas;*
- *Se $\phi$ é uma $\mathcal{L}$-formula, então para qualquer $p > 0$, $\forall v_p \phi$ e $\exists v_p \phi$ são $\mathcal{L}$-formulas;*
- *Qualquer $\mathcal{L}$-formula é obtida aplicando estas regras um numero finito de vezes.*

# Interpretação de Termos

Seja $A$ um conjunto. Definimos $A^\omega$ como:

$$A^\omega := \{(a_1, a_2, ...) : a_n \in A, \text{ para } n \geq 1\}$$

## Definição

*Seja $\mathcal{M}$ uma $\mathcal{L}$-estrutura e $t$ um $\mathcal{L}$-termo.*
*Definimos a interpretação de $t$ em $\mathcal{M}$ como a função:*

$$t^{\mathcal{M}} : M^\omega \to M$$

*Onde, para qualquer $\bar{a} \in M^\omega$, definimos:*

- *Se $t = v_p$, então $t^{\mathcal{M}}(\bar{a}) = a_p$;*
- *Se $t = c$, para $c \in \mathcal{C}$, então $t^{\mathcal{M}}(\bar{a}) = c^{\mathcal{M}}$;*
- *Se $t = f(t_1, ..., t_n)$. para $f \in \mathcal{F}_n$, então*

$$t^{\mathcal{M}}(\bar{a}) = f^{\mathcal{M}}(t_1^{\mathcal{M}}(\bar{a}), ..., t_n^{\mathcal{M}}(\bar{a}))$$

# Definição de Verdade de Tarski

## Definição

*Seja $\mathcal{M}$ uma $\mathcal{L}$-estrutura, $\phi$ uma $\mathcal{L}$-formula e $\bar{a} \in M^{\omega}$. Definimos $\mathcal{M} \models \phi[\bar{a}]$ como:*

- *Se $\phi$ é $t_1 = t_2$, então $\mathcal{M} \models \phi[\bar{a}]$ sse $t_1^{\mathcal{M}}(\bar{a}) = t_2^{\mathcal{M}}(\bar{a})$;*
- *Se $\phi$ é $R(t_1, ..., t_n)$ para $R \in \mathcal{R}_n$, então $\mathcal{M} \models \phi[\bar{a}]$ sse $(t_1^{\mathcal{M}}(\bar{a}), ..., t_n^{\mathcal{M}}(\bar{a})) \in R^{\mathcal{M}}$;*
- *Se $\phi$ é $\neg\psi$, então $\mathcal{M} \models \phi[\bar{a}]$ sse $\mathcal{M} \models \psi[\bar{a}]$ não é verdade;*
- *Se $\phi$ é $\psi \wedge \chi$, então $\mathcal{M} \models \phi[\bar{a}]$ sse $\mathcal{M} \models \psi[\bar{a}]$ e $\mathcal{M} \models \chi[\bar{a}]$;*
- *Se $\phi$ é $\psi \vee \chi$, então $\mathcal{M} \models \phi[\bar{a}]$ sse $\mathcal{M} \models \psi[\bar{a}]$ ou $\mathcal{M} \models \chi[\bar{a}]$;*
- *Se $\phi$ é $\psi \rightarrow \chi$, então $\mathcal{M} \models \phi[\bar{a}]$ sse $\mathcal{M} \models \psi[\bar{a}]$ implica $\mathcal{M} \models \chi[\bar{a}]$;*
- *Se $\phi$ é $\psi \leftrightarrow \chi$, então $\mathcal{M} \models \phi[\bar{a}]$ sse, $\mathcal{M} \models \psi[\bar{a}]$ sse $\mathcal{M} \models \chi[\bar{a}]$;*

# Definição de Verdade de Tarski

Dado $\bar{a} \in M^\omega$, $b \in M$ e $p \geq 1$, define-se $\bar{a}(p/b) \in M^\omega$ como o tuplo infinito obtido substituindo a $p$-ésima entrada por $b$:

$$\bar{a}(p/b) = (a_1, ..., a_{p-1}, b, a_{p+1}, ...)$$

## Definição (Continuação)

- *Se* $\phi$ *é* $\exists v_p \psi$, *então* $\mathcal{M} \models \phi[\bar{a}]$ *sse existe* $b \in M$ *tal que* $\mathcal{M} \models \psi[\bar{a}(p/b)]$;
- *Se* $\phi$ *é* $\forall v_p \psi$, *então* $\mathcal{M} \models \phi[\bar{a}]$ *sse para todo* $b \in M$ *temos* $\mathcal{M} \models \psi[\bar{a}(p/b)]$.

## Proposição

*Seja $\mathcal{M}$ uma $\mathcal{L}$-estrutura, $t$ um $\mathcal{L}$-termo e $\bar{a}, \bar{b} \in M^{\omega}$ tal que $a_p = b_p$ para todo $p \in \mathbb{N}$ tal que $v_p$ ocorre em $t$. Então*

$$t^{\mathcal{M}}(\bar{a}) = t^{\mathcal{M}}(\bar{b})$$

## Proposição

*Seja $\mathcal{M}$ uma $\mathcal{L}$-estrutura, $\phi$ uma $\mathcal{L}$-formula e $\bar{a}, \bar{b} \in \mathcal{M}^{\omega}$ tal que $a_p = b_p$ para todo $p \in \mathbb{N}$ tal que $v_p$ é uma variável livre em $\phi$. Então*

$$\mathcal{M} \models \phi[\bar{a}] \Leftrightarrow \mathcal{M} \models \phi[\bar{b}]$$

Uma fórmula sem variáveis livres chama-se uma sentença.

**Corolário**

*Seja $\mathcal{M}$ uma $\mathcal{L}$-estrutura e $\phi$ uma $\mathcal{L}$-sentença. Então apenas uma das seguintes é verdade:*

- $\mathcal{M} \models \phi[\bar{a}]$, *para todo* $\bar{a} \in M^{\omega}$;
- $\mathcal{M} \not\models \phi[\bar{a}]$, *para todo* $\bar{a} \in M^{\omega}$.

Se o primeiro caso acontecer, escrevemos $\mathcal{M} \models \phi$, e no segundo caso escrevemos $\mathcal{M} \not\models \phi$.

# Equivalência elementar

## Definição

*Sejam $\mathcal{M}, \mathcal{N}$ duas $\mathcal{L}$-estruturas. Dizemos que $\mathcal{M}$ é elementarmente equivalente a $\mathcal{N}$, que se denota por $\mathcal{M} \equiv \mathcal{N}$, se para qualquer $\mathcal{L}$-sentença $\phi$, temos*

$$\mathcal{M} \models \phi \Leftrightarrow \mathcal{N} \models \phi$$

## Proposição

*Se $\mathcal{M} \simeq \mathcal{N}$, então $\mathcal{M} \equiv \mathcal{N}$.*

**Nota**: $\mathcal{M} \equiv \mathcal{N} \not\Rightarrow \mathcal{M} \simeq \mathcal{N}$:
$(\mathbb{Q}, <) \equiv (\mathbb{R}, <)$, mas não há bijeções entre $\mathbb{Q}$ e $\mathbb{R}$.

## Proposição

*Se $\mathcal{M} \equiv \mathcal{N}$ são finitos, então $\mathcal{M} \simeq \mathcal{N}$.*

# Teorias

## Definição

*Seja $\mathcal{L}$ uma linguagem de primeira ordem. Uma $\mathcal{L}$-teoria $T$ é um conjunto de $\mathcal{L}$-sentenças.*

## Definição

*Seja $T$ uma $\mathcal{L}$-teoria e $\mathcal{M}$ uma $\mathcal{L}$-estrutura. Dizemos que $\mathcal{M}$ satisfaz $T$ ou que $\mathcal{M}$ é modelo de $T$, denotado por $\mathcal{M} \models T$ se $\mathcal{M} \models \phi$ para todo $\phi \in T$.*
*Se $T$ tem um modelo, dizemos que a teoria $T$ é satisfazível.*

# Exemplos

$\mathcal{L} = \emptyset$

$$\phi_n := \exists x_1 \exists x_2 ... \exists x_n \bigwedge_{i<j\leq n} x_i \neq x_j$$

Teoria dos conjuntos infinitos:

$$T = \{\phi_n : n \geq 1\}$$

# Exemplos

$\mathcal{L} = \{<\}$

Teoria dos conjuntos linearmente ordenados:

$$T = \{\forall x \neg(x < x),$$
$$\forall x \forall y \forall z((x < y \wedge y < z) \rightarrow x < z),$$
$$\forall x \forall y(x < y \wedge x = y \wedge x > y)\}$$

# Exemplos

$\mathcal{L} = \{E\}$

Teoria das relações de equivalência:

$$T = \{\forall x E(x,x),$$
$$\forall x \forall y (E(x,y) \rightarrow E(y,x)),$$
$$\forall x \forall y \forall z (E(x,y) \wedge E(y,z) \rightarrow E(x,z))\}$$

# Exemplos

$\mathcal{L} = \{\cdot, e\}$

Teoria dos grupos abelianos:

$$\begin{aligned} Grp = \{&\forall x(x \cdot e = x \wedge e \cdot x = x), \\ &\forall x \exists y(x \cdot y = e \wedge y \cdot x = e), \\ &\forall x \forall y \forall z((x \cdot y) \cdot z = x \cdot (y \cdot z)), \\ &\forall x \forall y(x \cdot y = y \cdot x)\} \end{aligned}$$

# Exemplos

$\mathcal{L} = \{+, \cdot, 0, 1\}$

Teoria dos anéis unitários:

$$\begin{aligned} \mathit{URng} = \mathit{Grp} \cup \{ & \forall x(x \cdot 1 = x \wedge 1 \cdot x = x), \\ & \forall x \forall y \forall z((x \cdot y) \cdot z = x \cdot (y \cdot z)), \\ & \forall x \forall y \forall z[x \cdot (y + z) = x \cdot y + x \cdot z], \\ & \forall x \forall y \forall z[(x + y) \cdot z = x \cdot z + y \cdot z]\} \end{aligned}$$

# Exemplos

$\mathcal{L} = \{+, \cdot, 0, 1\}$

Teoria dos corpos:

$$\mathit{Field} = \mathit{URng} \cup \{\forall x \forall y (x \cdot y = y \cdot x), \\ \forall x (x \neq 0 \rightarrow \exists y (x \cdot y = 1))\}$$

# Exemplos

$\mathcal{L} = \{+, \cdot, 0, 1\}$

Teoria dos corpos algebricamente fechados:
Para cada $n \geq 1$ seja

$$\phi_n := \forall a_0 ... \forall a_{n-1} \exists x \left( x^n + \sum_{i=0}^{n-1} x^i a_i = 0 \right)$$

$$ACF = Field \cup \{\phi_n : n \geq 1\}$$

# Exemplos

$\mathcal{L} = \{+, \cdot, 0, 1\}$

Para cada primo $p$ seja

$$\psi_p := \underbrace{1 + 1 + ... + 1}_{p} = 0$$

Se $F$ é um corpo, $F \models \psi_n$ sse $F$ tem característica $p$.

Teoria dos corpos algebricamente fechados de característica $p$ e 0:

$$ACF_p = ACF \cup \{\psi_p\}$$

$$ACF_0 = ACF \cup \{\neg\psi_p : p \geq 1\}$$

# $\mathrm{Th}(\mathcal{M})$

## Definição

*Seja $\mathcal{M}$ uma $\mathcal{L}$-estrutura. Definimos a teoria completa de $\mathcal{M}$ como:*

$$Th(\mathcal{M}) := \{\phi : \phi \text{ é uma } \mathcal{L}\text{-sentença e } \mathcal{M} \models \phi\})$$

## Proposição

*Sejam $\mathcal{M}, \mathcal{N}$ duas $\mathcal{L}$-estruturas. As seguintes são equivalentes:*

1. $\mathcal{M} \equiv \mathcal{N}$;
2. $Th(\mathcal{M}) = Th(\mathcal{N})$;
3. $\mathcal{N} \models Th(\mathcal{M})$;

# Consequência semântica

**Definição**

*Seja $T$ uma $\mathcal{L}$-teoria e $\phi$ uma $\mathcal{L}$-sentença. Dizemos que $\phi$ é consequencial semântica de $T$, denotado por $T \models \phi$, se para qualquer $\mathcal{L}$-estrutura $\mathcal{M}$, temos*

$$\mathcal{M} \models T \implies \mathcal{M} \models \phi$$

**Nota**: Se $T$ não é satisfazível, então $T \models \phi$ para qualquer sentença $\phi$.
Exemplos:

- $Grp \models \forall x(x \cdot x = x \to x = e)$
- $URng \not\models \forall x \forall y(x \cdot y = 0 \to (x = 0 \vee y = 0))$

# Teorema da Compacidade

Dizemos que uma $\mathcal{L}$-teoria $T$ é finitamente satisfazível se qualquer subconjunto finito de $T$ é satisfazível.

**Teorema (Teorema da Compacidade)**

*Seja $T$ uma $\mathcal{L}$-teoria. Então $T$ é satisfazível sse $T$ é finitamente satisfazível.*

**Nota**: A implicação

$$T \text{ satisfazível} \implies T \text{ finitamente satisfazível}$$

é trivial.

# Prova

**Definição**

*Seja $T$ uma teoria. Dizemos que $T$ é maximal se para qualquer sentença $\phi$, temos ou $\phi \in T$ ou $\neg\phi \in T$.*

**Definição**

*Seja $T$ uma teoria. Dizemos que $T$ tem testemunhas se para qualquer formula $\phi(v)$, existe um símbolo constante na linguagem $c$ tal que*

$$(\exists v \phi(v)) \rightarrow \phi(c) \in T$$

# Prova

**Lemma**

*Seja $T$ uma teoria maximal e finitamente satisfazível. Seja $\phi$ uma sentença e $\Delta \subseteq T$ um subconjunto finito. Então, se $\Delta \models \phi$, temos que $\phi \in T$.*

**Corolário**

*Seja $T$ uma teoria maximal, finitamente satisfazível e com testemunhas. Para qualquer formula $\phi(v)$, se $\exists v \phi(v) \in T$, então existe um símbolo constante $c$ tal que $\phi(c) \in T$.*

# Prova

O seguinte lema é a parte principal da prova:

**Lemma (Lema de Henkin)**

*Se $T$ é uma teoria finitamente satisfazível, maximal e com testemunhas. Então $T$ é satisfazível.*

A ideia para a prova do teorema da compacidade é então:

- Começar com uma teoria finitamente satisfazível $T$;
- Estender $T$ para $T'$ maximal, finitamente satisfazível com testemunhas;
- Obter modelo $\mathcal{M} \models T'$ pelo lema de Henkin;
- Como $T \subseteq T'$ então $\mathcal{M} \models T$.

# Prova

**Proposição**

*Seja $T$ uma $\mathcal{L}$-teoria finitamente satisfazível. Então existe uma $\mathcal{L}$-teoria $T'$ maximal finitamente satisfazível tal que $T \subseteq T'$.*

Precisamos dos seguintes 2 lemas:

**Lemma**

*Seja $T$ uma $\mathcal{L}$-teoria finitamente satisfazível e $\phi$ uma $\mathcal{L}$-sentença. Então ou $T \cup \{\phi\}$ é finitamente satisfazível, ou $T \cup \{\neg\phi\}$ é finitamente satisfazível.*

**Lemma (Zorn)**

*Seja $(X, \leq)$ um conjunto parcialmente ordenado. Se qualquer cadeia $C$ de elementos de $X$ tem um majorante em $C$, então $(X, \leq)$ tem um elemento maximal.*

# Prova

A peça final é próximo lema:

## Lemma (Lindenbaum)

*Seja $T$ uma $\mathcal{L}$-teoria finitamente satisfazível. Então existe uma linguagem $\mathcal{L}^* \supseteq \mathcal{L}$ e uma $\mathcal{L}^*$-teoria $T^* \supseteq T$ tal que:*

- *$T^*$ é finitamente satisfazível;*
- *Qualquer $\mathcal{L}^*$-teoria que estenda $T^*$ tem testemunhas.*

## Teorema

*Seja $T$ uma $\mathcal{L}$-teoria finitamente satisfazível. Então $T$ tem um modelo.*

# Exemplos de aplicações

**Proposição**

*Seja $T$ uma teoria que tem modelos finitos arbitrariamente grandes. Então $T$ tem um modelo infinito.*

**Proposição**

*Seja $\phi(v)$ uma formula na linguagem $\mathcal{L} = \{\cdot, e\}$ e seja $T \supseteq Grp$. Se para cada $n \geq 1$, existe $G_n \models T$ e $g_n \in G_n$ tal que $G_n \models \phi[g_n]$ e $g_n$ tem ordem pelo menos $n$, então existe $G \models T$ e $g \in G$ com ordem infinita tal que $G \models \phi[g]$.*

**Proposição**

*Um grupo $G$ é ordenável sse todo o subgrupo finitamente gerado de $G$ for ordenável.*

**Proposição**

*Um grafo é n-colorível sse todo o sub-grafo finito é n-colorível.*

# Exemplos de aplicações

**Proposição**

*Seja $T$ uma teoria de $\phi$ uma sentença. Então $T \models \phi$ sse existe $\Delta \subseteq T$ finito tal que $\Delta \models \phi$.*

Para cada $n \in \mathbb{N}$, seja

$$\phi_n = \exists x_1 ... \exists x_n \left( \bigwedge_{i<j\leq n} x_i \neq x_j \wedge \forall y \left( \bigvee_{i=1}^{n} y = x_i \right) \right)$$

Então $\mathcal{M} \models \phi_n$ sse $|M| = n$.
Será que existe uma formula $\phi_\infty$ tal que $\mathcal{M} \models \phi_\infty$ sse $\mathcal{M}$ é infinito?

**Corolário**

*Não existe nenhuma formula $\phi_\infty$ tal que $\mathcal{M} \models \phi_\infty$ se e só se $\mathcal{M}$ é infinito.*

# Ordinais

## Definição

*Um conjunto $X$ diz se transitivo se para qualquer $x \in X$, se $y \in x$ então $y \in X$.*
*Por outras palavras, $X$ é transitivo se $x \in X \Rightarrow x \subseteq X$*

Exemplos:

- $\{\emptyset, \{\emptyset\}\}$ é transitivo;
- $\{\{\emptyset\}\}$ não é transitivo.

## Definição

*Uma ordem total $<$ em $X$ diz-se uma boa ordem, se qualquer subconjunto de $X$ tiver um mínimo.*

Exemplos:

- $(\mathbb{R}, <)$ não é uma boa ordem;
- $(\mathbb{Z}, <)$ não é uma boa ordem;
- $(\mathbb{N}, <)$ é uma boa ordem.

# Ordinais

**Definição**

*Um conjunto $X$ é um ordinal se for transitivo, e bem ordenado pela relação $\in$.*
*A classe de todos os ordinais denota-se por $On$.*

Exemplos:

- $\emptyset$;
- $\{\emptyset\}$;
- $\{\emptyset, \{\emptyset\}\}$;
- $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$;
- $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\}$

# Ordinais

Notas:

- Sejam $\alpha, \beta$ ordinais. Se $\alpha \in \beta$, escrevemos $\alpha < \beta$;
- $(On, \in)$ é totalmente ordenado, i.e. dados dois ordinais $\alpha, \beta$, ou $\alpha \in \beta$, ou $\alpha = \beta$ ou $\beta \in \alpha$;
- $(On, \in)$ é bem ordenado, i.e. qualquer conjunto de ordinais tem um mínimo;
- Dado um ordinal $\alpha$, temos que $\alpha = \{\beta \in On : \beta < \alpha\}$.

# Ordinais

## Proposição

- *$\emptyset$ é um ordinal, e para todo o ordinal $\alpha$, ou $\alpha = \emptyset$ ou $\emptyset \in \alpha$, pelo que $\emptyset$ é o menor ordinal;*
- *Se $\alpha$ é um ordinal, $\alpha^+ := \alpha \cup \{\alpha\}$ é um ordinal, e se $\alpha \leq \beta \leq \alpha^+$, ou $\beta = \alpha$ ou $\beta = \alpha^+$;*
- *Se $C$ é um conjunto de ordinais, então $\bigcup_{\alpha \in C} \alpha$ é um ordinal e é o menor majorante de $C$, i.e. o seu supremo.*

# Ordinais

Exemplos:

- $0 := \emptyset$
- $1 := 0^+ = \{\emptyset\} \cup \emptyset = \{\emptyset\} = \{0\}$
- $2 := 1^+ = \{\{\emptyset\}\} \cup \{\emptyset\} = \{\emptyset, \{\emptyset\}\} = \{0, 1\}$
- $3 := 2^+ = \{\{\emptyset, \{\emptyset\}\}\} \cup \{\emptyset, \{\emptyset\}\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} = \{0, 1, 2\}$

  $\vdots$
- $\omega = \bigcup\{n : n = 0, 1, 2, 3, ....\} = \{0, 1, 2, 3, ....\}$

**Definição**

*Dizemos que um ordinal $\alpha$ é um ordinal sucessor se $\alpha = \beta^+$ para algum ordinal $\beta$.*
*Se $\alpha \neq 0$ e $\alpha$ não é um ordinal sucessor, dizemos que $\alpha$ é um ordinal limite.*

# Ordinais

**Teorema**

*Seja $(X, <)$ um conjunto bem ordenado. Então existe um único ordinal $\alpha$ isomorfo a $X$. Tal isomorfismo $f : (X, <) \to (\alpha, \in)$ é único. Neste caso, dizemos que a ordem de $X$ é do tipo $\alpha$, ou que o ordinal de $X$ é $\alpha$, e denotamos por $ord(X) = \alpha$.*

Exemplos:

- Se $(X, <)$ é um conjunto finito com $n$ elementos, então $ord(X) = n$;
- Se $X = (\mathbb{N}, <)$, então $ord(X) = \omega$.

# Ordinais

## Definição

*Sejam $\alpha$ e $\beta$ ordinais. Definimos $\alpha + \beta$ como sendo o ordinal de $(\{0\} \times \alpha) \cup (\{1\} \times \beta)$ com a ordem lexicográfica.*

Exemplos:

- $\omega + 1 = \omega^+$
- $1 + \omega = \omega$
- Para $n, m < \omega$, $n + m = m + n$

## Proposição

- $\alpha + 1 = \alpha^+$
- *Se $\alpha$ é infinito,* $1 + \alpha = \alpha$
- $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$
- $\alpha + 0 = \alpha = 0 + \alpha$

# Ordinais

## Definição

*Sejam $\alpha$ e $\beta$ ordinais. Definimos $\alpha \cdot \beta$ como sendo o ordinal de $\beta \times \alpha$ com a ordem lexicográfica.*

Exemplos:

- $\omega \cdot 2 = \omega + \omega$ ;
- $2 \cdot \omega = \omega$;

## Proposição

- $\alpha(\beta\gamma) = (\alpha\beta)\gamma$;
- $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$;
- $\alpha 1 = \alpha = 1\alpha$.

# Ordinais

## Definição

*Seja $\alpha$ um ordinal. Definimos:*

- $\alpha^0 = 1$
- $\alpha^{\beta^+} = \alpha^\beta \alpha$
- $\alpha^\beta = \sup\{\alpha^\gamma : \gamma < \beta\} = \bigcup_{\gamma<\beta} \alpha^\gamma$ *se $\beta$ é ordinal limite.*

Nota: Se $n < \omega$, então $\alpha^n = \underbrace{\alpha \cdot \ldots \cdot \alpha}_{n}$

# Ordinais

- $0, 1, 2, 3, 4, \ldots$
- $\omega$, $\omega + 1$, $\omega + 2$, $\omega + 3$,. . .
- $\omega + \omega = \omega 2$, $\omega 2 + 1$, $\omega 2 + 2$,. . .
- $\omega 3, \ldots, \omega 4, \ldots, \omega 5, \ldots$
- $\omega \cdot \omega = \omega^2, \ldots, \omega^3, \ldots, \omega^4, ..$
- $\sup\{\omega^n : n < \omega\} = \omega^\omega, \ldots, \omega^{\omega+1}, \ldots, \omega^{\omega+2}, \ldots$
- $\omega^{\omega 2}, \ldots, \omega^{\omega 3}, \ldots, \omega^{\omega^2}, \ldots, \omega^{\omega^\omega}, \ldots, \omega^{\omega^{\omega^\omega}}, \ldots$
- $\epsilon_0 = \sup\{\omega, \omega^\omega, \omega^{\omega^\omega}, \ldots\}$
- . . .

# Cardinais

## Teorema (Principio da boa ordenação)

*Seja $X$ um conjunto qualquer. Então existe uma relação de ordem total $<$ tal que $(X, <)$ é bem ordenado.*

## Definição

*Seja $X$ um conjunto qualquer. Definimos a cardinalidade de $X$, denotado por $|X|$, como sendo o ordinal.*

$$|X| = \min\{ord(X, <) : < \text{ é uma boa ordenação de } X\}$$

Exemplos/Notas:

- Se $X$ é finito e tem $n$ elementos, então $|X| = n$
- $|\mathbb{N}| = \omega$
- Dizemos que $X$ é numerável se $|X| = \omega$
- Todos os ordinais do slide anterior são numeráveis.

**Teorema**

*As seguintes são equivalentes:*

- $|X| \leq |Y|$;
- *Existe uma função injetiva* $f : X \to Y$

*As seguintes são equivalentes:*

- $|X| \geq |Y|$;
- *Existe uma função sobrejetiva* $f : X \to Y$

*As seguintes são equivalentes:*

- $|X| = |Y|$;
- *Existe uma função bijetiva* $f : X \to Y$

**Definição**

*Seja $\alpha$ um ordinal. Dizemos que $\alpha$ é um cardinal se $|\alpha| = \alpha$*

Exemplos/Notas:

- Se $X$ é um conjunto, $|X|$ é um cardinal.
- Qualquer ordinal finito é um cardinal
- $\omega$ é um cardinal
- $\omega_1 = \{\alpha \in On : \alpha \text{ é finito ou numerável}\}$ é o primeiro cardinal infinito não numerável.

# Cardinais

## Definição

*Definimos $\omega_\alpha$ para $\alpha \in On$ recursivamente como:*

- $\omega_0 = \omega$
- $\omega_{\alpha+1} = \{\delta \in On : |\delta| = \omega_\alpha\}$
- *Se $\alpha$ é ordinal limite, $\omega_\alpha = \sup_{\beta<\alpha} \omega_\beta$*

## Proposição

- *Para cada $\alpha \in On$, $\omega_\alpha$ é um cardinal*
- *$\omega_\alpha < \omega_\beta$ se e só se $\alpha < \beta$*
- *Se $\kappa$ é um cardinal, então ou $\kappa$ é finito ou $\kappa = \omega_\alpha$ para algum $\alpha \in On$*

Notas:

- Quando estamos a pensar em $\omega_\alpha$ como cardinal, é comum denotar por $\aleph_\alpha$.
- $\aleph_0, \aleph_1, \aleph_2, ..., \aleph_\omega, ...$

**Definição**

*Seja $\alpha$ um cardinal, i.e. $\alpha = \aleph_\beta$ para algum ordinal $\beta$. Definimos os sucessor de $\alpha$ denotado por $\alpha^+$ como sendo $\aleph_{\beta+1}$.*
*Um cardinal diz que cardinal sucessor se for o sucessor de algum cardinal. Se um cardinal diferente de 0 não for sucessor, dizemos que é cardinal limite.*

Notas:

- Todos os cardinais sucessores são ordinais limite.

# Cardinais

## Definição

*Sejam* $\kappa = |X|$ *e* $\lambda = |Y|$ *cardinais . Definimos:*

- $\kappa + \lambda = |\{0\} \times X \cup \{1\} \times Y|$
- $\kappa\lambda = |X \times Y|$
- $\kappa^\lambda = |X^Y| = \{f : f \text{ é uma função } Y \to X\}$

## Proposição

- *Se* $\kappa$ *e* $\lambda$ *são finitos, estas operações coincidem com as operações usuais da aritmética.*
- *Caso contrario,* $\kappa + \lambda = \kappa\lambda = \max\{\kappa, \lambda\}$
- $(\kappa^\lambda)^\mu = \kappa^{\lambda\mu}$
- *Se* $|I| \leq \kappa$ *e* $|A_i| \leq \kappa$ *então* $|\bigcup_{i \in I} A_i| \leq \kappa$
- *Se* $\lambda$ *é infinito e* $2 \leq \kappa < \lambda$*, então* $2^\lambda = \kappa^\lambda = \lambda^\lambda$

# Cardinais

Nota: Dado um conjunto $X$ com $|X| = \kappa$, então $|\mathcal{P}(X)| = |2^X| = 2^{|X|} = 2^\kappa$.

**Teorema**

*Seja $\kappa$ um cardinal. Então $\kappa < 2^\kappa$.*

Exemplo: $\mathfrak{c} = |\mathbb{R}| = |]0,1[| = 10^{\aleph_0} = 2^{\aleph_0} > \aleph_0$

**Hipótese do Contínuo**

$2^{\aleph_0} = \aleph_1$

**Hipótese do Contínuo Generalizada**

$2^{\aleph_\alpha} = \aleph_{\alpha+1}$, *Para qualquer ordinal $\alpha \in On$.*

# Mapas Elementares

**Definição**

*Sejam $\mathcal{M}$ e $\mathcal{N}$ duas $\mathcal{L}$-estruturas. Um mapa $f : M \to N$ diz-se elementar se para qualquer $\mathcal{L}$-formula $\phi(v_1, ..., v_n)$ e para qualquer $\bar{a} \in M^n$ temos*

$$\mathcal{M} \models \phi[\bar{a}] \Leftrightarrow \mathcal{N} \models \phi[f(\bar{a})]$$

Notas:

- Qualquer isomorfismo é um mapa elementar;
- Qualquer mapa elementar é um mergulho;
- Se existe um mapa elementar $f : \mathcal{M} \to \mathcal{N}$, então $\mathcal{M} \equiv \mathcal{N}$.

# Extensões Elementares

## Definição

*Sejam $\mathcal{M} \leq \mathcal{N}$ duas $\mathcal{L}$-estruturas. Dizemos que $\mathcal{M}$ é uma subestrutura elementar de $\mathcal{N}$, ou que $\mathcal{N}$ é uma extensão elementar de $\mathcal{M}$, denotado por $\mathcal{M} \preceq \mathcal{N}$, se a inclusão $\iota : \mathcal{M} \hookrightarrow \mathcal{N}$ for um mapa elementar, i.e. para qualquer $\mathcal{L}$-formula $\phi(v_1, ..., v_n)$ e $a_1, ..., a_n \in M$:*

$$\mathcal{M} \models \phi[a_1, ..., a_n] \Leftrightarrow \mathcal{N} \models \phi[a_1, ..., a_n]$$

# Teorema de Löwenheim–Skolem para baixo

## Teorema (Löwenheim–Skolem para baixo)

*Seja $\mathcal{M}$ uma $\mathcal{L}$-estrutura, $X \subseteq M$ um conjunto potencialmente vazio. Então, para qualquer cardinal infinito $\lambda$ tal que*

$$|X| + |\mathcal{L}| \leq \lambda \leq |M|$$

*Existe uma subestrutura elementar $\mathcal{N}$ de $\mathcal{M}$ com cardinalidade $\lambda$ tal que $X \subseteq N$.*

# Diagrama Elementar

Dada uma $\mathcal{L}$-estrutura $\mathcal{M}$, $\mathcal{L}_M$ denota a linguagem obtida de $\mathcal{L}$ adicionando um símbolo constante para cada $m \in M$.

## Definição

*Dada uma $\mathcal{L}$-estrutura $\mathcal{M}$, definimos:*

- *O seu diagrama atómico como*

$$Diag_{at}(\mathcal{M}) = \{\phi : \phi \text{ é uma } \mathcal{L}_M\text{-sentença atómica e } \mathcal{M} \models \phi\}$$

- *O seu diagrama elementar como*

$$Diag(\mathcal{M}) = \{\phi : \phi \text{ é uma } \mathcal{L}_M\text{-sentença e } \mathcal{M} \models \phi\}$$

# Diagrama Elementar

**Proposição**

*Seja $\mathcal{M}$ uma $\mathcal{L}$-estrutura e $\mathcal{N}$ uma $\mathcal{L}_M$-estrutura. Então:*

- *Se $\mathcal{N} \models Diag_{at}(\mathcal{M})$, então existe um mergulho $j : \mathcal{M} \hookrightarrow \mathcal{N}$;*
- *Se $\mathcal{N} \models Diag(\mathcal{M})$, então existe um mergulho elementar $j : \mathcal{M} \hookrightarrow \mathcal{N}$.*

**Nota**: No primeiro caso temos então que $\mathcal{M} \leq \mathcal{N}$ e no segundo caso temos $\mathcal{M} \preceq \mathcal{N}$.

# Teorema de Löwenheim–Skolem para cima

**Teorema (Löwenheim–Skolem para cima)**

*Seja $\mathcal{M}$ uma $\mathcal{L}$-estrutura infinita e $\lambda$ um cardinal infinito tal que*

$$|M| + |\mathcal{L}| \leq \lambda$$

*Então existe uma extensão elementar de $\mathcal{M}$ com cardinalidade $\lambda$.*

# Completude

**Definição**

*Uma teoria satisfazível $T$ diz-se completa se todos os modelos de $T$ são elementarmente equivalentes.*

Exemplo: Dado uma estrutura $\mathcal{M}$, então $\mathrm{Th}(\mathcal{M})$ é completa pois se $\mathcal{N}, \mathcal{K} \models \mathrm{Th}(\mathcal{M})$, então $\mathcal{N} \equiv \mathcal{M} \equiv \mathcal{K}$.

**Proposição**

*Seja $T$ uma teoria satisfazível. Então $T$ é completa sse para qualquer sentença $\phi$, temos $T \models \phi$ ou $T \models \neg\phi$.*

# Categoricidade

## Definição

*Seja $T$ uma teoria e $\kappa$ um cardinal infinito. Dizemos que $T$ é $\kappa$-categórica se tem pelo menos um modelo de cardinalidade $\kappa$ e quaisquer dois modelos de cardinalidade $\kappa$ são isomorfos.*

## Teorema (Teste de Vaught)

*Seja $T$ uma $\mathcal{L}$-teoria satisfazível sem modelos finitos. Se $T$ é $\kappa$-categórica para algum $\kappa \geq \max\{|\mathcal{L}|, \aleph_0\}$, então $T$ é completa.*

# Exemplos

Seja $(X, <)$ um conjunto linearmente ordenado.
Dizemos que $(X, <)$ é denso se

$$\forall x \forall y (x < y \rightarrow \exists z (x < z < y))$$

Dizemos que $(X, <)$ não tem extremidades se

$$\forall x \exists a \exists b (a < x < b)$$

A teoria dos conjuntos linearmente ordenados, densos e sem extremidades denota-se por $DLO$.

**Teorema (Teorema do isomorfismo de Cantor)**

*Quaisquer dois conjuntos numeráveis linearmente ordenados, densos e sem extremidades são isomorfos, i.e. DLO é $\aleph_0$-categórica.*

# Exemplos

**Corolário**

*DLO é completa.*

Então, por exemplo $(\mathbb{Q}, <) \equiv (\mathbb{R}, <) \equiv (\mathbb{R}^n, <_{lex})$

Mais exemplos de teorias categóricas:

- $ACF_p$ é $\kappa$-categórica para $k > \aleph_0$, para $p$ primo ou $p = 0$;
- A teoria dos grupos abelianos divisíveis livres de torção é $\kappa$-categórica para $\kappa > \aleph_0$;
- A teoria dos espaços vetoriais sobre um corpo contável fixo é $\kappa$-categórica para $\kappa > \aleph_0$

Pelo teste de Vaught, estas são todas completas.

# Aplicações

**Proposição**

*Seja $T$ uma teoria de $\phi$ uma sentença. Então $T \models \phi$ sse existe $\Delta \subseteq T$ finito tal que $\Delta \models \phi$.*

Relembrar:

$$\text{Seja } \psi_p := \underbrace{1 + 1 + ... + 1}_{p} = 0$$

$$ACF_p := ACF \cup \{\psi_p\}$$

$$ACF_0 := ACF \cup \{\neg\psi_p : p \geq 1\}$$

# Aplicações

## Teorema (Principio de Lefschetz)

*Seja $\mathcal{L} = \{\cdot, +, -, 0, 1\}$ e $\phi$ uma $\mathcal{L}$-sentença. As seguintes são equivalentes:*

1. $\mathbb{C} \models \phi$;
2. $ACF_0 \models \phi$;
3. $\phi$ *é verdade em algum ACF de característica* 0.
4. *Existem primos arbitrariamente grandes p, tal que* $\phi$ *é verdade em algum ACF de característica p;*
5. *Existe um natural m tal que para qualquer primo* $p \geq m$, $ACF_p \models \phi$.

# Aplicações

**Teorema (Ax–Grothendieck)**

*Qualquer mapa polinomial injetivo de $\mathbb{C}^n$ para $\mathbb{C}^n$ é sobrejetivo.*

$\phi_{2,2} =$

$$\forall a_{0,0}\forall a_{0,1}\forall a_{0,2}\forall a_{1,0}\forall a_{1,1}\forall a_{2,0}\forall b_{0,0}\forall b_{0,1}\forall b_{0,2}\forall b_{1,0}\forall b_{1,1}\forall b_{2,0}$$
$$\Big[\big(\forall x_1\forall y_1\forall x_2\forall y_2((\sum a_{i,j}x_1^i y_1^j = \sum a_{i,j}x_2^i y_2^j \wedge \sum b_{i,j}x_1^i y_1^j = \sum b_{i,j}x_2^i y_2^j) \rightarrow$$
$$(x_1 = x_2 \wedge y_1 = y_2))\big) \rightarrow \forall u\forall v\exists x\exists y \sum a_{i,j}x^i y^j = u \wedge \sum b_{i,j}x^i y^j = v\Big].$$

# Conjuntos Definíveis

## Definição

*Seja $\mathcal{M}$ uma $\mathcal{L}$-estrutura e $A \subseteq M$. Dizemos que $X \subseteq M^n$ é $A$-definível se existe uma $\mathcal{L}$-formula $\phi(v_1, ..., v_n, w_1, ..., w_m)$ e $a_1, ..., a_m \in A$ tal que*

$$X = \{\bar{x} \in M^n : \mathcal{M} \models \phi[x_1, ..., x_n, a_1, ..., a_m]\}$$

*Neste caso, dizemos que $\phi$ define $X$ com parâmetros em $A$, e denotamos*

$$X = \phi(\mathcal{M}, \bar{a})$$

*onde $\bar{a} \in A^m$ são os parâmetros fixos utilizados.*

# Conjuntos Definíveis

## Definição

*Seja $\mathcal{M}$ uma $\mathcal{L}$-estrutura e $A \subseteq M$.*

- *Dizemos que uma relação n-ária $R$ é $A$-definível se é $A$-definível enquanto conjunto $R \subseteq M^n$.*
- *Dizemos que um mapa $f : M^n \to M^m$ é $A$-definível, se o seu gráfico $\Gamma(f) = \{(x, f(x)) : x \in M^n\} \subseteq M^n \times M^m$ for $A$-definível.*
- *Dizemos que $x \in M^n$ é $A$-definível se $\{x\}$ é $A$-definível.*

# Exemplos

- $\mathcal{M} = (\mathbb{R}, +, \cdot, 0, 1)$. Seja $p(x) = a_n x^n + ... + a_1 x + a_0$. Então

$$\{x \in \mathbb{R} : p(x) = 0\}$$

é $\{a_0, ..., a_n\}$-definível.

- $\mathcal{M} = (\mathbb{R}, +, \cdot, 0, 1)$.

$$\phi(a, b) = \exists z(z \neq 0 \wedge b = a + z^2)$$

Então $< = \{(x, y) : \mathcal{M} \models \phi[x, y]\}$ ou seja $x < y$ sse $\mathcal{M} \models \phi[x, y]$. Então $<$ é uma relação $\emptyset$-definível.

- $\mathcal{M} = (\mathbb{R}, +, \cdot, 0, 1)$

$$\phi(a, b) = 0 \leq a \wedge b \leq 0 \wedge a = b^2$$

Então a função $x \mapsto \sqrt{x}$ é $\emptyset$-definível. O seu gráfico é $\{(x, y) : \mathcal{M} \models \phi[x, y]\}$.

# Exemplos

- $\mathcal{M} = (\mathbb{R}, +, \cdot, 0, 1)$. Se $q \in \mathbb{Q}$, então $q$ é $\emptyset$-definível.

Teorema de Lagrange: Qualquer inteiro não negativo é a soma de 4 quadrados.

- $\mathcal{M} = (\mathbb{Z}, +, \cdot, 0, 1)$. A formula

$$\phi(a, b) = \exists z_1 \exists z_2 \exists z_3 \exists z_4 (z_1 \neq 0 \wedge b = a + z_1^2 + z_2^2 + z_3^2 + z_4^2)$$

  define a ordem $<$ em $\mathbb{Z}$.
- Seja $F$ corpo e $\mathcal{M} = (F[X], +, \cdot, 0, 1)$. $F$ é $\emptyset$-definível pela forma

$$\phi(x) = (x = 0 \vee \exists y \ xy = 1)$$

  pois $F = U(F[X])$

# Exemplos

- $\mathcal{M} = (\mathbb{Q}, +, \cdot, 0, 1)$. Seja

$$\phi(x, y, z) = \exists a \exists b \exists c (xyz^2 + 2 = a^2 + xy^2 - yc^2)$$

No artigo "How to Pick Out the Integers in the Rationals: An Application of Number Theory to Logic"os autores mostraram que a fórmula

$$\psi(x) = \forall y \forall x([\phi(y, z, 0) \wedge (\forall w(\phi(y, z, w) \rightarrow \phi(y, z, w + 1)))] \rightarrow \phi(y, z, x))$$

Define $\mathbb{Z}$.

# Conjuntos Definíveis

## Proposição

*Seja $\mathcal{M}$ uma $\mathcal{L}$-estrutura, e $X, Y \subseteq M^n$ conjuntos $A$ e $B$-definíveis respetivamente. Então:*

- *$M^n \setminus X$ é $A$-definível;*
- *$X \cap Y$ é $(A \cup B)$-definível;*
- *$X \cup Y$ é $(A \cup B)$-definível;*

# Conjuntos Definíveis

## Proposição

*Seja $\mathcal{M}$ uma $\mathcal{L}$-estrutura e $X \subseteq M^n$ um conjunto $A$-definível. Então qualquer $\mathcal{L}$-automorfismo de $\mathcal{M}$ que fixe $A$ ponto a ponto (i.e. $f(a) = a$ para todo $a \in A$), fixa $X$ enquanto conjunto (i.e. $f(X) = X$).*

## Corolário

$\mathbb{R}$ *não é definível em* $(\mathbb{C}, +, \cdot, 0, 1)$

**Proof** If $\mathbb{R}$ were definable, then it would be definable over a finite $A \subset \mathbb{C}$. Let $r, s \in \mathbb{C}$ be algebraically independent over $A$ with $r \in \mathbb{R}$ and $s \notin \mathbb{R}$. There is an automorphism $\sigma$ of $\mathbb{C}$ such that $\sigma|A$ is the identity and $\sigma(r) = s$. Thus, $\sigma(\mathbb{R}) \neq \mathbb{R}$ and $\mathbb{R}$ is not definable over $A$.

# Eliminação de Quantificadores (EQ)

## Definição

*Seja $T$ uma $\mathcal{L}$-teoria. Dizemos que $T$ tem eliminação de quantificadores (EQ) se, para qualquer $\mathcal{L}$-fórmula $\phi(v_1, ..., v_n)$ existe uma $\mathcal{L}$-fórmula $\psi(v_1, ..., v_n)$ sem quantificadores tal que*

$$T \models \forall \bar{v}(\phi(\bar{v}) \leftrightarrow \psi(\bar{v}))$$

Exemplos:

- $\phi(a, b, c) = \exists x(a \neq 0 \wedge ax^2 + bx + c = 0)$ Então

$$\mathbb{R} \models \forall a \forall b \forall c(\phi(a, b, c) \leftrightarrow (a \neq 0 \wedge b^2 - 4ac \geq 0))$$

- Seja

$$\phi(a, b, c, d) = \exists x \exists y \exists u \exists v \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x & y \\ u & v \end{pmatrix} = Id$$

Então

$$F \models \forall a \forall b \forall c \forall d(\phi(a, b, c, d) \leftrightarrow ad - bc \neq 0)$$

# Critérios para EQ

**Teorema**

*Seja $T$ uma $\mathcal{L}$-teoria. Se para qualquer fórmula sem quantificadores $\theta(\bar{v}, w)$ existe uma fórmula sem quantificadores $\phi(\bar{v})$ tal que*

$$T \models (\exists w \theta(\bar{v}, w)) \leftrightarrow \phi(\bar{v})$$

*Então $T$ tem eliminação de quantificadores.*

# Critérios para EQ

Uma fórmula é um literal se for ou uma fórmula atómica, ou a negação de uma fórmula atómica.

**Definição**

*Uma fórmula sem quantificadores diz se uma conjunção básica se for da forma* $\bigwedge_{i=1}^{n} \phi_i$ *Onde cada* $\phi_i$ *é um literal.*

**Proposição**

*Qualquer formula sem quantificadores* $\phi$ *é equivalente a uma disjunção finita de conjunções básicas.*

Relembrar:

- $\exists x(\phi \vee \psi)$ é equivalente a $(\exists x\phi) \vee (\exists x\psi)$;
- $\forall x(\phi \wedge \psi)$ é equivalente a $(\forall x\phi) \wedge (\forall x\psi)$.

# Critérios para EQ

## Teorema

*Seja $T$ uma $\mathcal{L}$-teoria. Se para qualquer conjunção básica $\theta(\bar{v}, w)$ existe uma fórmula sem quantificadores $\phi(\bar{v})$ tal que*

$$T \models (\exists w \theta(\bar{v}, w)) \leftrightarrow \phi(\bar{v})$$

*Então $T$ tem eliminação de quantificadores.*

## Teorema

*As seguintes teorias tem eliminação de quantificadores:*

- *Teoria dos conjuntos infinitos;*
- *DLO;*
- *Grupos abelianos divisíveis livres de torção;*
- *Grupos abelianos divisíveis ordenados;*

# *EQ* em *DLO*

- O que são as conjunções básicas em DLO?
- Como vão ser os termos?

$$t(v_1, \ldots, v_n) = v_i$$

- Então as formulas atómicas vão ser da forma:

$$v_i = v_j$$
$$v_i < v_j$$

- Os literais vão ser então da forma:

$$v_i = v_j$$
$$v_i < v_j$$
$$\neg(v_i = v_j)$$
$$\neg(v_i < v_j)$$

# $EQ$ em $DLO$

- Seja $\phi(v_1, \ldots, v_n, y)$ conjunção básica.

$$\exists y \phi(v_1, \ldots, v_n, y) = \exists y \bigwedge_{i=1}^{k} \theta_i(v_1, \ldots, v_n, y)$$

$$\downarrow$$

$$\exists y \phi = \exists y \Big[ \bigwedge_{i \in I} (y = v_i) \wedge \bigwedge_{j \in J} (y < v_j) \wedge \bigwedge_{k \in K} (v_k < y) \wedge \bigwedge_{i' \in I'} \neg(y = v_{i'}) \wedge \bigwedge_{j' \in J'} \neg(y < v_{j'}) \wedge \bigwedge_{k' \in K'} \neg(v_{k'} < y) \Big]$$

Onde $I, J, K, I', J', K' \subseteq \{1, \ldots, n\}$

# *EQ* em *DLO*

Notar:

- $\neg(y = v_{i'})$ é equiv. a $y < v_{i'} \vee v_{i'} < y$;
- $\neg(y < v_{j'})$ é equiv. a $y = v_{j'} \vee v_{i'} < y$;
- $\neg(v_{k'} < y)$ é equiv. a $y = v_{k'} \vee y < v_{k'}$.

Então podemos assumir que

$$\exists y \phi = \exists y \left[ \bigwedge_{i \in I} (y = v_i) \wedge \bigwedge_{j \in J} (y < v_j) \wedge \bigwedge_{k \in K} (v_k < y) \right]$$

Para $I, J, K \subseteq \{1, \ldots, n\}$.

Caso 1: $I = \emptyset$ Então

$$\exists y \phi = \exists y \left[ \bigwedge_{j \in J} (y < v_j) \wedge \bigwedge_{k \in K} (v_k < y) \right]$$

Considerar

$$\psi(v_1, \ldots, v_n) = \begin{cases} v_1 = v_1 & \text{se } J = \emptyset \text{ ou } K = \emptyset \\ \bigwedge_{j \in J, k \in K} (v_k < v_j) & \text{cc.} \end{cases}$$

Caso 2: $I \neq \emptyset$

$$\exists y \phi = \exists y \left[ \bigwedge_{i \in I} (y = v_i) \wedge \bigwedge_{j \in J} (y < v_j) \wedge \bigwedge_{k \in K} (v_k < y) \right]$$

Seja $t \in \{v_i : i \in I\}$. Tomamos

$$\psi(v_1, \ldots, v_n) = \bigwedge_{i \in I} t = v_i \wedge \bigwedge_{j \in J} t < v_j \wedge \bigwedge_{k \in K} v_k < t$$

# Aplicações

## Definição

*Uma $\mathcal{L}$-teoria $T$ é model-complete se, dados $\mathcal{M}, \mathcal{N} \models T$ com $\mathcal{M} \leq \mathcal{N}$, então $\mathcal{M} \preceq \mathcal{N}$.*
*Por outras palavras, todos os mergulhos são elementares.*

## Proposição

*Se $T$ tem eliminação de quantificadores, então $T$ é model-complete.*

# Aplicações: ACF

**Teorema**

*ACF tem eliminação de quantificadores em $\mathcal{L}_r$.*

**Corolário**

*ACF é model-complete.*

**Corolário**

*Para qualquer $p$ primo ou $p = 0$, $ACF_p$ é model-complete e completo.*

# Geometria Algébrica 101

Seja $K \models ACF$ um corpo.

## Definição

*Para* $S \subseteq K[X_1, ..., X_n]$, *definimos*

$$V(S) = \{\bar{a} \in K^n : p(\bar{a}) = 0, \text{ para todo } p \in S\}$$

*Dizemos que* $X \subseteq K^n$ *é um fechado de Zariski se* $X = V(S)$ *para algum* $S \subseteq K[X_1, ..., X_n]$.

Exemplos:

- $V(1) = \emptyset$
- $V(0) = K^n$
- $V(\{X_1 - a_1, ..., X_n - a_n\}) = \{(a_1, ..., a_n)\}$

Nota: Dois polinómios diferentes podem gerar o mesmo conjunto: $V(x) = V(x^2)$

## Proposição

- *$V$ é decrescente: $S \subseteq S' \implies V(S) \supseteq V(S')$;*
- *$V(S) = V(\langle S \rangle)$ onde*

$$\langle S \rangle = \left\{ \sum_{finita} a_i f_i : f_i \in S \text{ e } a_i \in K[X_1, ..., X_n] \right\}$$

- *Dado $S \subseteq K[X_1, ..., X_n]$, existem $f_1, ..., f_k \in \langle S \rangle$ tal que $V(S) = V(f_1, ..., f_k)$;*
- *Dados $S_i \subseteq K[X_1, ..., X_n]$,*

$$\bigcap_{i \in I} V(S_i) = V\left( \bigcup_{i \in I} S_i \right)$$

- *Uniões finitas de fechados de Zariski são fechados de Zariski.*

## Definição

*Para $X \subseteq K^n$, definimos*

$$I(X) = \{p \in K[X_1, ..., X_n] : p(\bar{a}) \text{ para todo } \bar{a} \in X\}$$

## Proposição

- *$I$ é decrescente: $X \subseteq Y \implies I(X) \supseteq I(Y)$;*
- *$I(X)$ é um ideal;*
- *Se $X$ é fechado de Zariski, então $V(I(X)) = X$;*
- *$J \subseteq I(V(J))$, mas a igualdade em geral não é verdade.*

Exemplo:
Se $J = \langle x^2 \rangle$, então $V(\langle x^2 \rangle) = \{0\}$ e portanto $I(V(\langle x^2 \rangle)) = \langle x \rangle$.

# Aplicações

**Lemma**

*Os subconjuntos definíveis por fórmulas atómicas em $K^n$ são exatamente os conjuntos da forma $V(p)$ para algum $p \in K[X_1, ..., X_n]$.*
*Um subconjunto de $K^n$ é definido por uma fórmula sem quantificadores se e só se é combinação booleana de fechados de Zariski.*

Na literatura, um subconjunto de $K^n$ que é uma combinação booleana de fechados de Zariski chama-se um **conjunto construível**.

**Teorema (Teorema de Chevalley)**

*A imagem de um conjunto construível por um mapa polinomial é construível.*

# Aplicações

Relembrar:

## Definição

*Seja $R$ um anel e $I$ um ideal. O radical de $I$ é o ideal*

$$\sqrt{I} = \{x \in R : x^n \in I \text{ para algum } n \in \mathbb{N}\}$$

*$I$ é um ideal radical se $\sqrt{I} = I$.*

Notas:

- Dado $X \subseteq K^n$, $I(X)$ é sempre um ideal radical.
- Dado um ideal $J$ de $K[X_1, \ldots, X_n]$, $V(\sqrt{J}) = V(J)$

## Definição

*Seja $R$ um anel. Um ideal $P$ diz-se primo se, dados dois ideais $I, J$ com $IJ \subseteq P$, então $I \subseteq P$ ou $J \subseteq P$.*

# Aplicações

## Teorema (Decomposição Primária)

*Seja $I \subseteq K[X_1, ..., X_n]$ um ideal radical. Então existem ideais primos únicos $P_1, ..., P_k$ com $I \subseteq P_i$, tal que:*

- $I = P_1 \cap ... \cap P_k$;
- *Para qualquer $J \subsetneq \{1, ..., k\}$, $I \neq \bigcap_{j \in J} P_j$.*

## Teorema (Hilbert's Nullstellensatz)

*Seja $K$ algebricamente fechado e $I, J \subseteq K[X_1, \ldots, X_n]$ ideais radicais. Se $I \subsetneq J$, então $V(J) \subsetneq V(I)$.*
*Em particular, o mapa $X \mapsto I(X)$ é uma correspondência bijetiva entre os fechados de Zariski e ideais radicais.*

## Corolário

*Seja $K$ algebricamente fechado e $J$ um ideal radical. Então $I(V(J)) = J$.*